SIMON TOUCH

User Manual

Motorola Key Tool

SIMON TOUCH

Overview

This software and accompanied drivers are intended for educational purposes only and it's use is sole liability of user. All further consequences of any other possible device use is subject of user's choice and responsibility.

The drivers, provided are original Cypress® inf-file and original Cypress® library files, which compatibility to Your current operating system is subject of Cypress® technical notes and bulletins. Any further questions of misbehaved CyUSB-library to be forwarded to Cypress® Support Desk.

Hardware serial number is visible in Windows in “My Computer” / “Properties” / “Hardware” / “Device Manager” - selecting the device - “Properties” / “Details” / “Device Instance id” and Serial Number (8 digits and/or characters) is shown after VID and PID of the interface hardware. The method, described above may vary, depending on exact operation system You are using, but in general is the same. This unique serial number eases identification of Your hardware in manufacturer database, providing You corresponding initial software and further updates.

Hardware contains Lithium battery for backing up the critical data for supporting it's functionality. Do not use / store the device in extreme temperatures or inappropriate humidity or another operational conditions, as this could lead to big leakage currents, shortening battery life. Consult Lithium-battery specifications for proper storage and usage. In any case it is good idea to have device connected and powered by USB port or another external compatible +5V DC source for prolonging battery lifespan.

SIMON TOUCH

How to use

At start of the software, if hardware is properly connected, You will see the following (button/labels if not active, this means You did something wrong):

Always mind the exact order of connecting and disconnecting the Motorola/interface/PC – not following might seriously harm any/all components:

1. Solder Motorola MCU to adapter board
2. Plug Motorola adapter board to Motorola Key Tool hardware in proper direction. See below photo – DO NOT reverse adapter board !!! When connecting adapter board, Motorola Key Tool should be disconnected from USB – always mind that !!!
3. Connect hardware to available USB port of PC.

Upon completion of Your work with Motorola Key Tool disconnect in the reverse order:

1. Unplug Motorola Key Tool hardware from USB port of PC.
2. Disconnect Motorola adapter board Motorola Key Tool hardware.
3. Unsolder Motorola MCU from adapter board.

After that step, You could plug again Motorola Key Tool to USB, even if not used. It's important for it's battery maintenance to be powered most of the time. Disconnect it from USB when PC has being switched off to avoid transient power peaks on USB connector power supply when computer has been powered on.

SIMON TOUCH

Here is shown proper connection of adapter board to Motorola Key Tool:

As visible from photo, the orientation of adapter board should be facing up to the label of Motorola Key Tool. Also photo shows, that Motorola MCU soldered to adapter board should be free of dirt, soldering paste and any other flux, which might interfere with electrical signals. Have the adapter well cleared after soldering, using Isopropyl alcohol or another suitable cleaning solution.

Press “Read” button to check if You did required and above described connection.

The data shown is:

“Key” - Key number. Any MB has eight keys and this information helps to

identify current one from the others in the set. Many car settings of seats, mirrors, steering wheel position and more are matched to this number.

"SSID" - hexadecimal representation of MB **S**ystem **S**erial **Id**entifier. Identifies key to **EIS** - Electronic Ignition Switch, **ICM** - Instrument Cluster Module, **CGW** - Central Gateway, **ESL** - Electronic Steering Lock , **ECU** - Electronic Control Unit for the engine or transmission modules - "7G-Tronic" (**ETC**), **ISM**, etc... modules, which are related to **FBS®** (immobilizer) system.

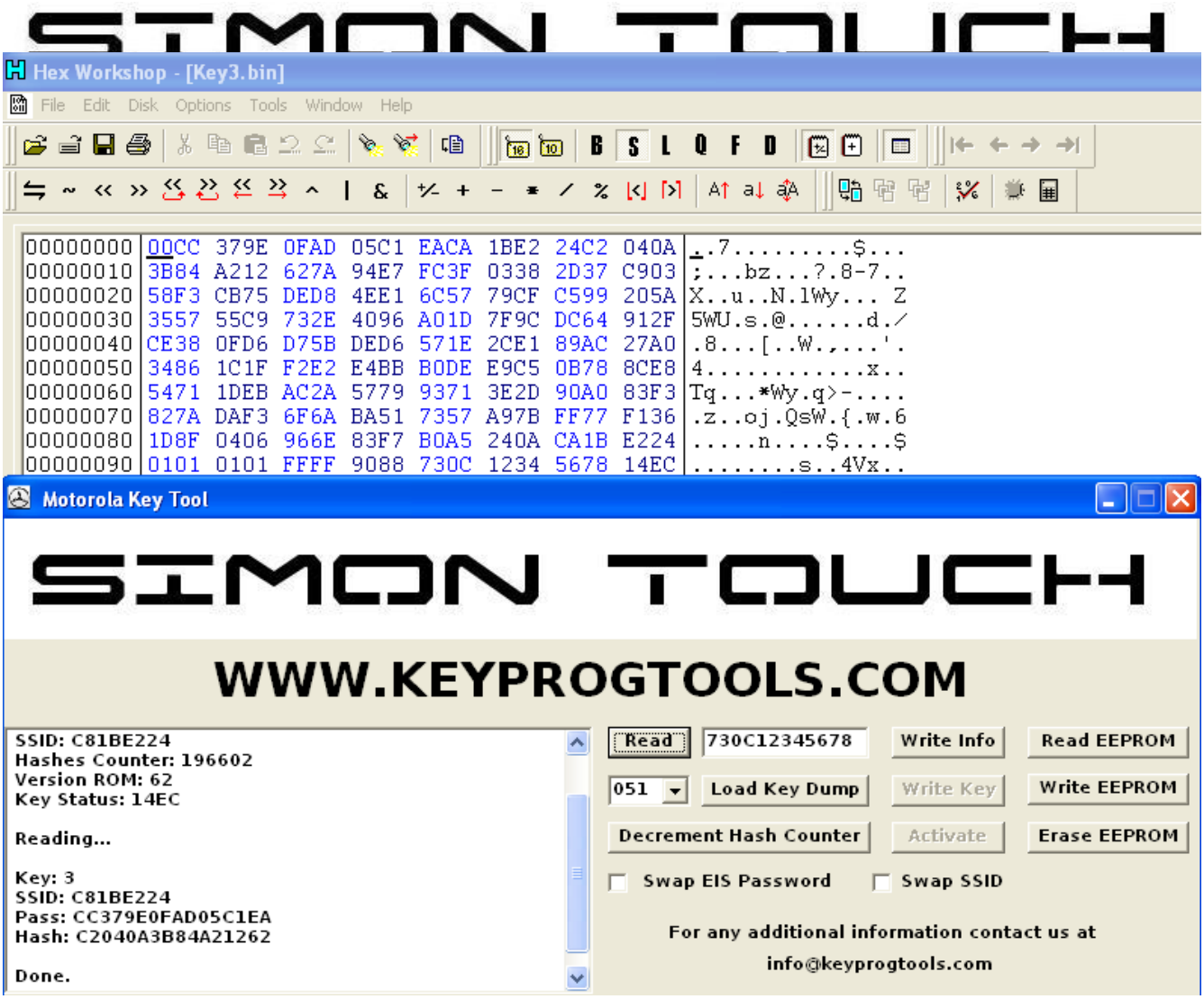
"Hashes Counter" - remaining starts counter – it is same as Hashes counter of EIS hashes, and both decrement together when MB key is inserted into EIS. Initial value is 196607 when MB key is new and decrements when MB key is used. Differences in "Hashes Counter" of EIS and MB key could occur and this leads to car unable to start if key counter is bigger than EIS hash counter.
Solution is in Your hands and it is simple using Motorola Key Tool to adjust key counter same or little lesser then EIS counter!!! For this purpose You should click button "Decrement Hashes Counter" as many times as You need. Read further for an example. This function emulates inserting key to EIS with all data being exchanged as car does. Do not "play" with this button – if key counter becomes too lesser than EIS hash counter key will become non operational. There is a margin of 100 counts (in general) which EIS tolerates for difference in "Hashes Counter".

"Version ROM" - version of software, programmed in Motorola MCU.

"Key Status" - hexadecimal representation of internal operational state. Two bytes completes to number of 0x100 (in most common example for Key it is 0x14 + 0xEC=0x100). If that check-sum fails, Motorola MCU becomes inoperative. Following is description of most common Status digits:

0000 – MB Key is blank (erased state of Key after production).
21DF – MB Key is prepared (Key accepts only encrypted data).
04FC – MB Key is programmed, but not activated.
05FB – MB Key is programmed, but not activated.
14EC – MB Key is activated and fully functional.
15EB – MB Key is activated and fully functional.
0CF4 – MB Key for service purposes (so called "Green Key").

You could also read internal EEPROM data by clicking "Read EEPROM"


Hex Workshop - [Key3.bin]
File Edit Disk Options Tools Window Help
00000000 00CC 379E 0FAD 05C1 EACA 1BE2 24C2 040A
00000010 3B84 A212 627A 94E7 FC3F 0338 2D37 C903
00000020 58F3 CB75 DED8 4EE1 6C57 79CF C599 205A
00000030 3557 55C9 732E 4096 A01D 7F9C DC64 912F
00000040 CE38 0FD6 D75B DED6 571E 2CE1 89AC 27A0
00000050 3486 1C1F F2E2 E4BB B0DE E9C5 0B78 8CE8
00000060 5471 1DEB AC2A 5779 9371 3E2D 90A0 83F3
00000070 827A DAF3 6F6A BA51 7357 A97B FF77 F136
00000080 1D8F 0406 966E 83F7 B0A5 240A CA1B E224
00000090 0101 0101 FFFF 9088 730C 1234 5678 14EC
Motorola Key Tool
SIMON TOUCH
WWW.KEYPROGTOOLS.COM
SSID: C81BE224
Hashes Counter: 196602
Version ROM: 62
Key Status: 14EC
Reading...
Key: 3
SSID: C81BE224
Pass: CC379E0FAD05C1EA
Hash: C2040A3B84A21262
Done.
Read
730C12345678
Write Info
Read EEPROM
051
Load Key Dump
Write Key
Write EEPROM
Decrement Hash Counter
Activate
Erase EEPROM
Swap EIS Password
Swap SSID
For any additional information contact us at
info@keyprogtools.com

After few seconds (not immediate – it takes time) EEPROM content is displayed. Above screen-shot is showing data read according to the file being programmed previously to the Motorola MCU.

Information, being read data is automatically saved in two of the most popular formats for bin-files, related to MB. File, sized of 512 bytes is for SKC® software and another file, sized 57 bytes is for server calculations. Two folders are created by software - “read” and “archive”. Inside “read” folder You will find all Motorola MCUs, read by You, saved in above mentioned two formats. Every Motorola MCU file is named by it's unique SSID. So, it is very easy to identify the needed data and process it further. Every time same Motorola MCU is read file is filled with the latest data read, so You do not need to worry about file validity. For

tracking any changes of Motorola MCU data, second folder “archive” contains all tries to read any Motorola. Files are named by Key unique SSID with added date

and hour, so it's very easy to roll back the data to any specific moment You need it. Also this guarantees that newer files will not replace the older ones. This "archive" folder could grow with time, so have a look at it regularly and clean it if not necessary data is contained.

Except above described files, automatically produced by software, You will be given a choice to save 160-bytes EEPROM content of Motorola MCU in folder and under name You type in appropriate Save dialog box.

After Password and Hash data are read and shown on screen, be sure that You have read corresponding EIS first and You have all Keys Hashes, numbered from 1 to 8, and also so called "Service Hash" (also called "Dealer Password" or different, depending on people's habit to name it). All these records (Hashes and SSID) are needed for further calculation of new Key for the car or adapting other modules – in example ESL for W203. Have in mind, that first You should use our IR Tool software to read EIS Hashes, which are vital part of Mercedes Benz ® FBS immobilizer system and You can't use Motorola Key Tool files only for direct generation of all EIS Keys content. With data read by Motorola Key Tool for current Key, You can only duplicate that specific Key, but for making another Key or adapting ESL You should have complete data for car, read from EIS.

You shouldn't bother for files saving, matching, etc... All that is done automatic by both IR Tool and Motorola Key Tool software if they are in same folder.

First IR Tool creates file, named by EIS SSID and fills it with Hashes data. After You read Motorola Key MCU for that EIS, Motorola Key Tool just inserts Password data in the same file. And ONLY after that You could process the files to SKC® software or server for generating Keys content. Those steps are important and shouldn't be mistaken if You need complete files for any EIS/Key set.

If You just need to read Password / Initial Hash from Key then use Motorola Key Tool software only and proceed further with data provided by it.

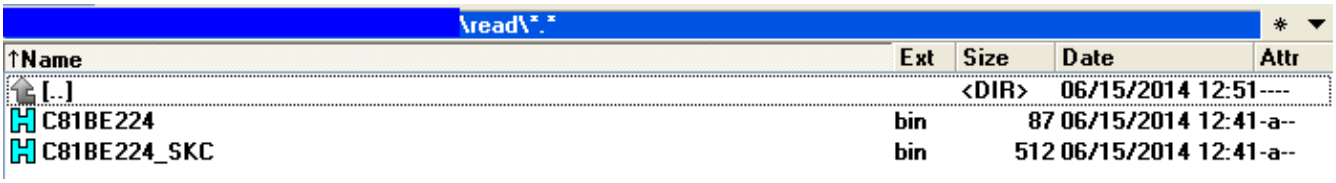
Note: Check or un-check "Swap EIS Password" and "Swap SSID" depending on file format that Your key processing software requires!!!

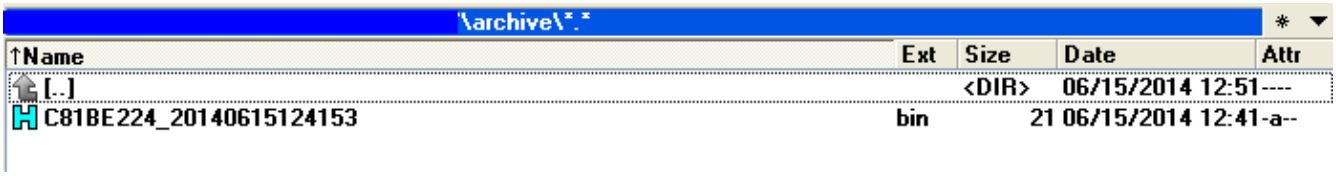
In general, You shouldn't bother about these two check-boxes. Software takes care about automatically swapping data being written to Motorola MCU when "Write Key" button is used, but Your experience will show if swap the data or not. Most of the existing key generating solutions require these to be blank.

Here are examples of folders / files structure for produced results after reading of a single Motorola MCU and how saved files match to data being

programmed to the specific key.

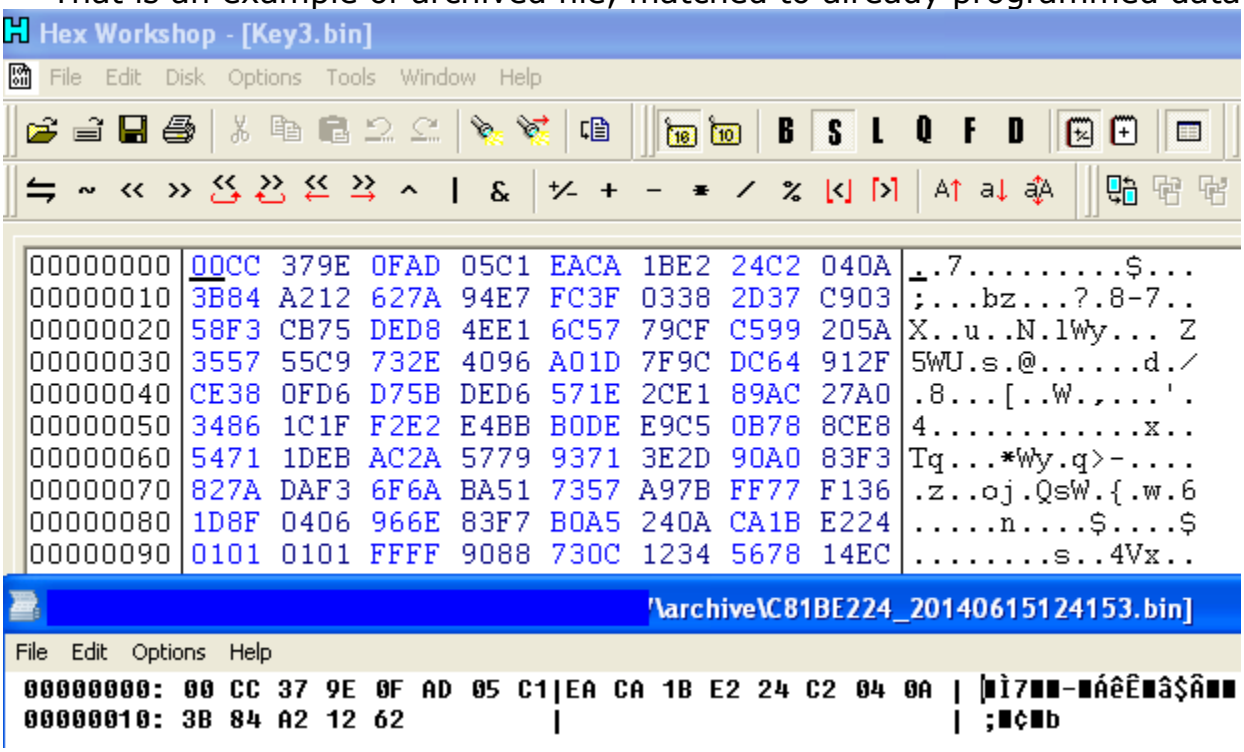
That is the content of “read” folder:





That is the content of “archive” folder:

That is an example of archived file, matched to already programmed data:



If You need to make new Key for the car, using complete data, already read from original Key, then proceed further those files and have Your Key set files generated. Exit Motorola Key Tool software, disconnect it from USB and remove adapter board from it to unsolder original Motorola MCU.

It is supposed, that You will want to keep that original Key and will not erase it or overwrite it with another Key data. But if You want to do such to it – for example if You want to change it's Key number, because of corrupted Hash data for current one, then just leave it on board and proceed further.

But if You want to keep it intact, then solder either blank or another used Motorola MCU to adapter board for writing new Key content to it. Connect the boards and hardware as already described! Start Motorola Key Tool software and if needed erase the new Motorola MCU, by clicking “Erase EEPROM”.

When done, software will inform You:

ONLY now You could write new Key content to Motorola MCU. Do not proceed directly to writing if You are not sure if it is erased. Spent few seconds to erase EEPROM. If You skip this important step and You will have to repeat it from beginning if writing operation returns error.

Note: You have two options: “Write EEPROM” button, which writes complete 160-byte EEPROM of MCU or “Write Key” button, which writes Key with commands, as it happens via IR channel.

If You use "Write EEPROM" button selected files goes directly to Motorola EEPROM and is not needed to explain anything.

Note, that most right 3 buttons "Read EEPROM", "Erase EEPROM" and "Write EEPROM" are acting like device programmer in a kind of ETL, UPA or similar – they do raw byte to byte operation. No commands involved, no checksums, nothing... simple byte to byte reading / erasing / writing...

If You use "Write Key" button for writing data to Motorola EEPROM it happens in MB way as performed via IR channel and is explained further.

Select appropriate Motorola Key file format – 011, 021, 041 or 051. In general these namings are by last digits of Motorola MCU marking i.e. MA 567 880 041. Press "Load Key Dump" button to check if You did proper file format selection. Preliminary information for the Key dump content will be displayed, showing You "Key Number", "SSID" and "Hashes Counter", contained in the file. Wrong Key file format, not corresponding to MCU being programmed results in errors – always check MCU mask!

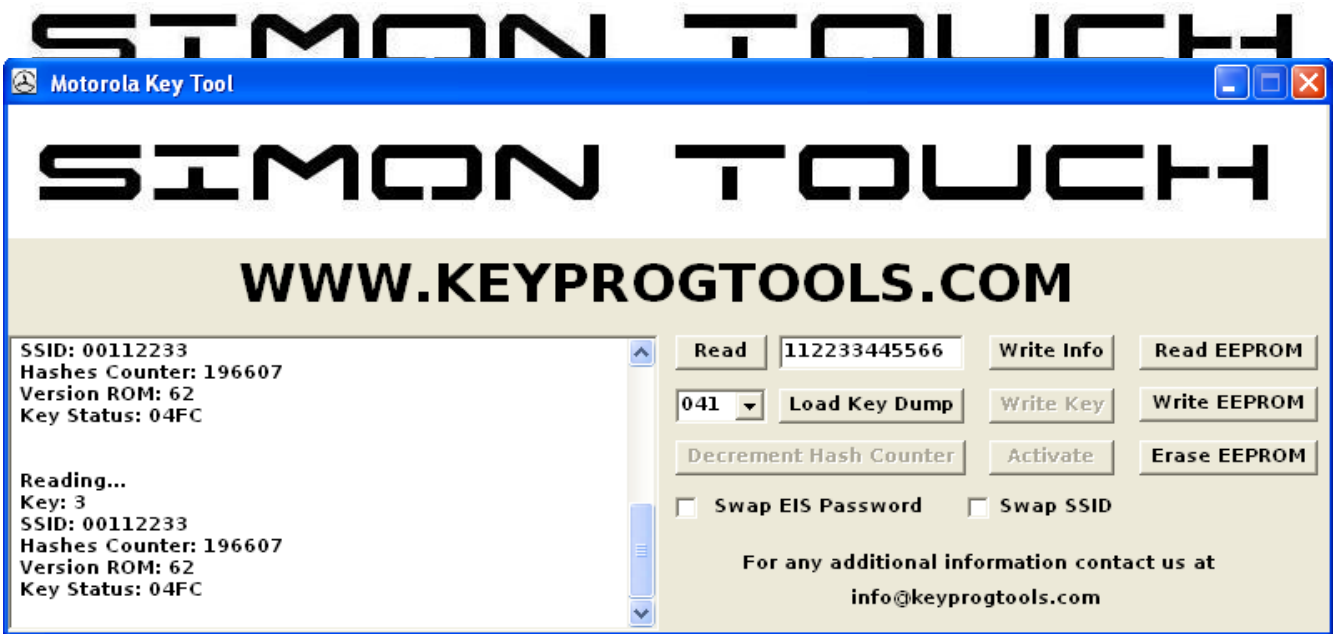
Proceed with "Write Key" and software will inform You for completion of it:

Screenshot shows You error if default "051" file format remains and how after selecting the right format "041" writing process completes properly!

Always mind this MCU file format and change it to corresponding to Motorola chip, You are working on. There are a lot of Motorola chips masks, so be careful and always adjust file format selection !!!

Now You could check the result of writing procedure by clicking “Read”:

If You want, You could also write “Info Bytes” field. The writing is possible not only after that step, but at any moment – it's just shown here. For example change their values from “000000000000” shown above to “112233445566”. Fill the corresponding field with desired data and click the button “Write Info” right next to it. Check the result after by clicking “Read”:



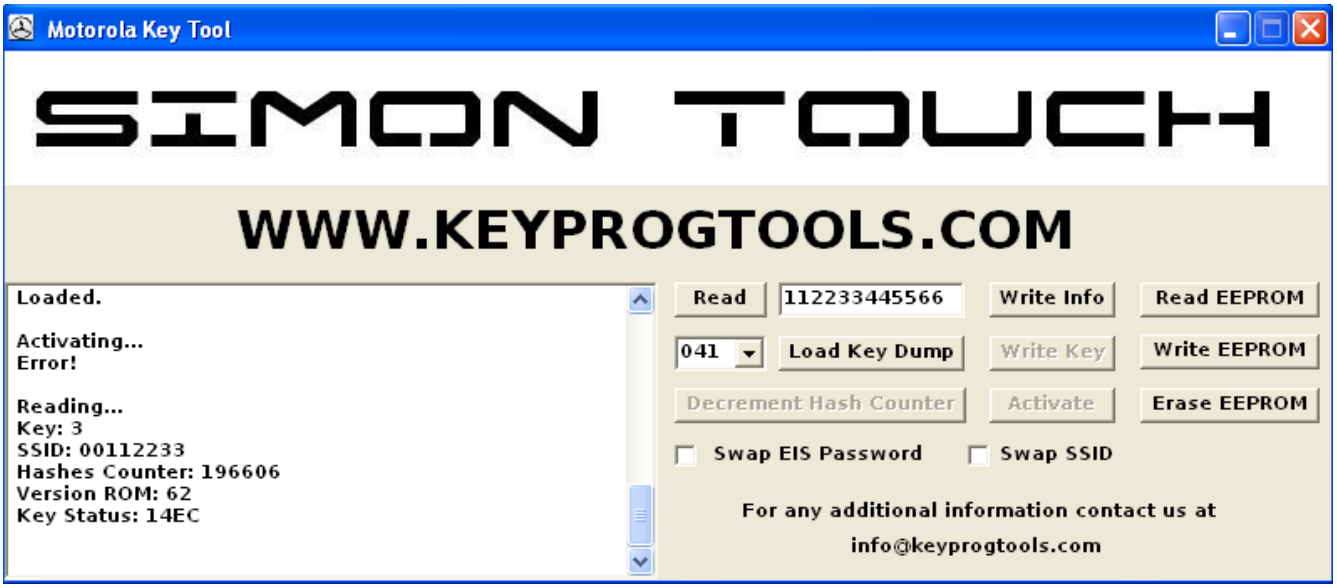
If the Key Number You just programmed to Motorola MCU is "not used" in EIS, then You are done and could exit the software, disconnect the hardware from USB and unsolder Motorola MCU from adapter board for further soldering back to Key PCB and using in car.

But if You programmed Key Number which has it's status "used" in EIS, then You should activate it first and then decrement it's counter to match the EIS Hashes counter. Click "Activate" - note that this button could be used only if You load corresponding EEPROM dump for that Key.

Give the software needed time to complete that operation and check it's

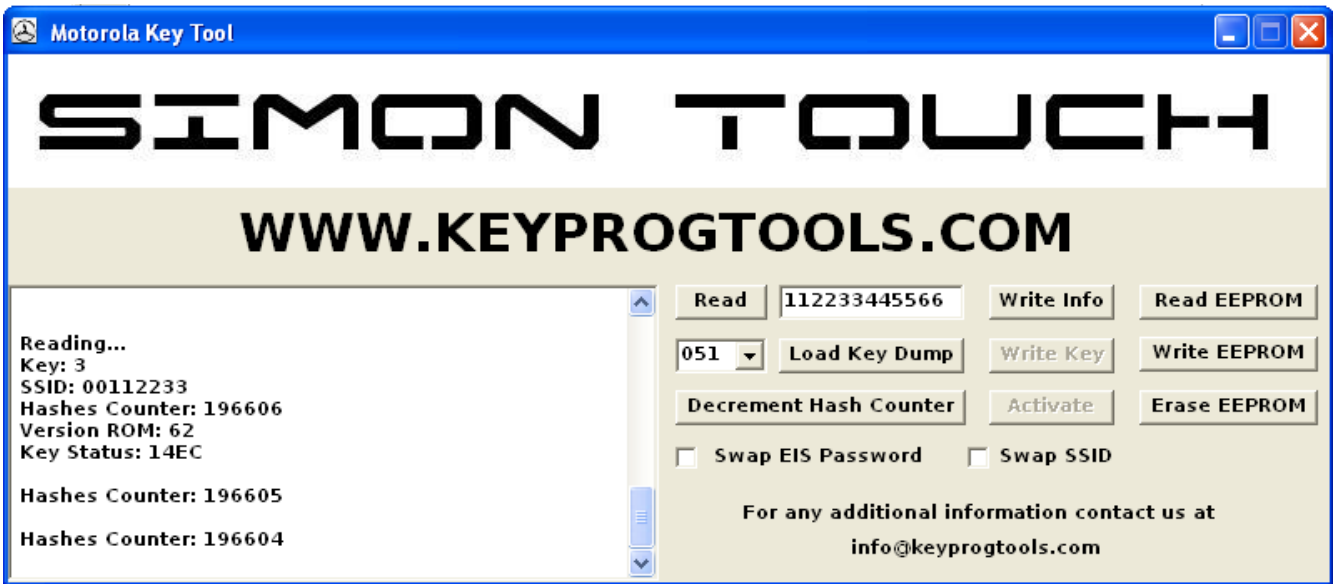
result, despite the messages software produces:

Now the "Key Status" has changed from "04FC" to "14EC" and "Hashes Counter" has been decremented in activation process. If You need that counter even less than value displayed, the You should use "Decrement Hashes Counter" button. Click it and it shades – when completed it will be active again:



Decrementing process is time-consuming, because of Hashes reordering in

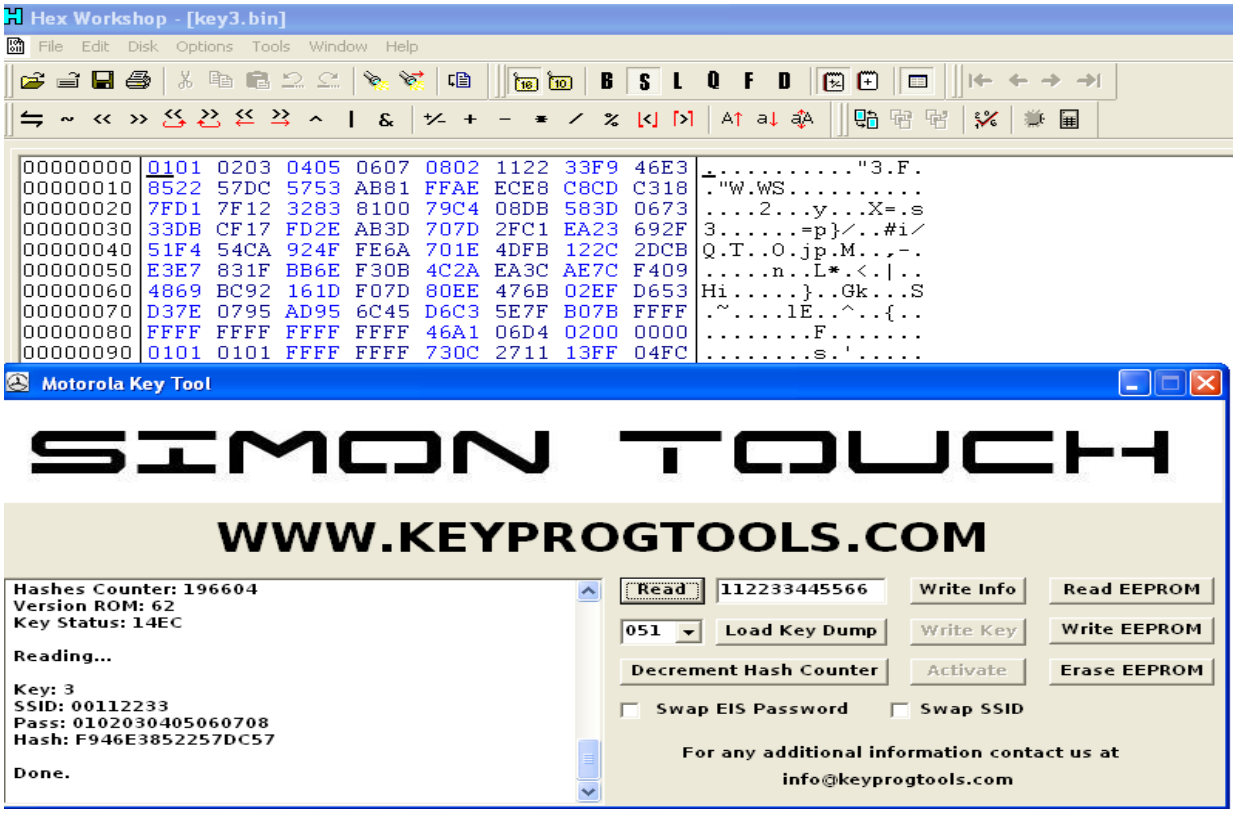
Motorola MCU EEPROM, so wait for it to finish. Do not interrupt it! It's important for EEPROM integrity this process to finish correct! Software will give You new "Hashes Counter" value:



You could check it again by clicking "Read":

You could check also (not needed, but if You like it...) the correctness of whole programming process by reading EEPROM Bytes:

SIMON TOUCH


Hex Workshop - [key3.bin]
File Edit Disk Options Tools Window Help
00000000 0101 0203 0405 0607 0802 1122 33F9 46E3
00000010 8522 57DC 5753 AB81 FFAE ECE8 C8CD C318
00000020 7FD1 7F12 3283 8100 79C4 08DB 583D 0673
00000030 33DB CF17 FD2E AB3D 707D 2FC1 EA23 692F
00000040 51F4 54CA 924F FE6A 701E 4DFB 122C 2DCB
00000050 E3E7 831F BB6E F30B 4C2A EA3C AE7C F409
00000060 4869 BC92 161D F07D 80EE 476B 02EF D653
00000070 D37E 0795 AD95 6C45 D6C3 5E7F B07B FFFF
00000080 FFFF FFFF FFFF FFFF 46A1 06D4 0200 0000
00000090 0101 0101 FFFF FFFF 730C 2711 13FF 04FC
Motorola Key Tool
SIMON TOUCH
WWW.KEYPROGTOOLS.COM
Hashes Counter: 196604
Version ROM: 62
Key Status: 14EC
Reading...
Key: 3
SSID: 00112233
Pass: 0102030405060708
Hash: F946E3852257DC57
Done.
Read
112233445566
Write Info
Read EEPROM
051
Load Key Dump
Write Key
Write EEPROM
Decrement Hash Counter
Activate
Erase EEPROM
Swap EIS Password
Swap SSID
For any additional information contact us at
info@keyprogtools.com

Enjoy it !!!